

CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

1. I, Geoffrey Yandl, a Special Agent of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), being duly sworn, depose and state as follows:
2. I have been an ATF Special Agent since 2007. My duties include the investigation of various violations of federal criminal law, including matters involving violations of 18 U.S.C. § 922, which makes it illegal to possess firearms as a prohibited person, to include being previously convicted of a crime punishable by more than a year of incarceration, hereinafter, the “Subject Offense”.
3. I make this Continuation of Application for a Search Warrant in support of a warrant to search the person, property, or premises identified in Attachment A for the items and evidence identified in Attachment B. As set forth below, there is probable cause to believe a search of the person, property, or premises identified in Attachment A will reveal evidence of the Subject Offenses.
4. This continuation is based on the investigation, observations, and/or experience of ATF Special Agent Geoffrey Yandl, as well as other law enforcement officers. I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses will be revealed during a search of the person, property, or premises identified in Attachment A.

BACKGROUND OF INVESTIGATION

5. Theretius A. GREENBERRY, date of birth XX/XX/2000, resides in Muskegon, MI. Agent Yandl conducted a LEIN inquiry and learned that GREENBERRY has 14 arrests. GREENBERRY has juvenile adjudications for Felony Armed Robbery, Felony Larceny, and Felony Assault of a Prison Employee. In 2018, as an adult, GREENBERRY pleaded No Contest to a Felony Firearm Offense and received two years in prison. GREENBERRY was discharged

from the Michigan Department of Corrections on the maximum penalty without parole on February 15, 2020.

6. On or about May 20, 2020, the Michigan State Police (MSP) received information that the SnapChat account for Theretius GREENBERRY, identified as username **Ckurry93**, posted a video. Detective Dillard Hayes obtained a copy of the video. The video showed two subjects in a wooded area firing handguns. One of the subjects is believed to be GREENBERRY based on physical likeness. The video is titled, “Big ass Glokk inis Bih wont jam” with three laughing face emojis.

7. On or about May 22, 2020, MSP received information that GREENBERRY’s SnapChat account, **Ckurry93**, posted a video of GREENBERRY. Detective Hayes obtained a copy of the video. The video shows a close up of GREENBERRY waiving a black handgun, pointing the handgun at the camera and talking about shooting at houses. GREENBERRY stated in the video that he is not “high”. He gives his address as 277 Irwin and says “You know where I stay at”. This is a still picture from the video:



8. On June 4, 2020, at approximately 7:00pm, MSP received information that a SnapChat account screenname **Billygang19**, utilized by Amari Smith-Bryant, posted a video. Detective Hayes obtained a copy of the video. The video shows Smith-Bryant and GREENBERRY dancing and singing. GREENBERRY is waiving a black handgun around and pointing it at the camera. The video is titled, "Ktfu I'm drunk". This is a still picture from the video:



9. On June 4, 2020, at approximately 10:15pm, MSP uniform troopers assigned to Muskegon obtained information from the Violent Crimes Task Force that GREENBERRY was riding in a white Chevrolet Tahoe armed with a handgun.

- a. MSP located the subject vehicle and determined that it was operating without proper insurance. A traffic stop was conducted and contact was made with the driver. The driver was unable to provide proof of insurance and the vehicle became

subject to impound. MSP made contact with the passenger and identified him as GREENBERRY.

- b. Upon conducting an inventory search of the vehicle, troopers located a black handgun partially hidden under the passenger seat. On the center console troopers found a bag of suspected ecstasy pills.
 - i. The firearm is specifically described as a loaded black Glock, Model 21, .45 caliber semiautomatic pistol with serial number BCKS279.
 - ii. Your affiant, through training and experience in the determination of firearms travelling through interstate commerce, advises that that firearm was distributed from the State of Georgia. Therefore, the firearm traveled through interstate commerce prior to its possession by GREENBERRY.
- c. In a post-Miranda statement, the driver stated that earlier in the day he was at a house with GREENBERRY. GREENBERRY showed the driver the handgun. The driver said GREENBERRY also has several pictures of the handgun on his phone.
- d. GREENBERRY was detained and advised of his rights pursuant to Miranda. He declined to make a statement without an attorney present.
- e. When officers searched GREENBERRY incident to his arrest, they located two Apple iPhones on him. These phones are currently in the custody of the Michigan State Police.
 - i. One is further described as a black iPhone, Model Number A1660, in a black case with a cracked screen.
 - ii. The other is further described as a black iPhone, Model Number A1661, with a clear case.

**BACKGROUND ON MESSAGING APPLICATIONS
GENERALLY, AND SNAPCHAT SPECIFICALLY**

10. Instagram, Twitter, Facebook, Snapchat, and text messaging are common tools used by mobile devices with access to the Internet, such as smart phones or tablets. Users of Instagram, Twitter, Snapchat, and Facebook must register a password protected account which they can access with a smartphone data plan or Wi-Fi Internet access to send and receive messages, photographs, videos, sketches, mobile webpages, and other content. Oftentimes, with a smartphone that has a data plan with a wireless provider, users of these social media platforms can use text messages services included in their phone plan to send and receive messages, photographs, videos, sketches, mobile webpages, and other content, just as happens through social media accounts.

11. The social media accounts are often used as a platform to maintain an online social media profile which can be viewed by "friends" or "followers" and they can use their online profile to share photographs and videos or engage in chat sessions, meet other people, among other things. While posting status updates, comments, or likes on their profile, social media users can allow others to view their profiles or keep them private. Since social media accounts can contain location data and are commonly viewed by peers, more personal communication can occur with direct messaging through the social media application, or through text messages.

12. The Snapchat Law Enforcement Guide, published by Snapchat, Inc., and last updated September 21, 2018, states that "Snapchat is a mobile application made by Snap Inc. ("Snap") and available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats." The Guide also lists some of the information that is or may be available by way of valid process served on Snap Inc. According to Snap Inc., this information includes, but is not limited to the following:

- a. Subscriber Information: to include Snapchat username, E-mail address, phone number, display name, Snapchat account creation date and IP address, timestamp and IP address of account logins and logouts.
- b. Logs of Previous Snaps, Stories, and Chats: logs contain metadata about a user's Snaps, Stories, and Chats, but not the user's content.
- c. Content: In certain limited circumstances, content of sent Snaps and chat content may be available. Memories content may be available until deleted by a user.
- d. The Law Enforcement Guide defines Snapchat features as follows:
- e. Snaps: Snaps are photos or videos taken using the Snapchat app's camera on an individual's mobile device, and may be shared directly with the user's friends, or in a Story (explained below) or Chat. Snap's servers are designed to automatically delete a Snap after it has been viewed by all intended recipients. Snap's servers are designed to automatically delete an unopened Snap sent directly to a recipient after 30 days and an unopened Snap in Group Chat after 24 hours.
- f. Stories: A user can add Snaps to their "Story". A Story is a collection of Snaps displayed in chronological order. Users can manage their privacy settings so that their Story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to our crowd-sourced service "Our Story", which enables their Snaps to be viewed by all Snapchatters in Search and Snap Map. Snap's servers are designed to automatically delete a Snap in a user's Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to Our Story may be saved for longer periods of time.

- g. **Memories:** Memories is Snapchat’s cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone’s photo gallery in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called “My Eyes Only”), in which case the content is not accessible to Snap and cannot be decrypted by Snap.
- h. **Chat:** A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature. Our servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user’s chat settings. Snap’s servers are designed to automatically delete unopened one-to-one chats in 30 days. Users can also chat in groups. Chats sent in groups are deleted after 24 hours whether they are opened or not. A user can save a message in Chat by pressing and holding the message. The user can unsave the message by pressing and holding it again. This will delete it from our servers. Users can also delete chats that they have sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat.
- i. **Location Data:** If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user’s use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

**REQUEST FOR AUTHORIZATION TO
UNLOCK DEVICES WITH FINGERPRINTS OR FACE ID**

13. Based on my knowledge and experience, I know that certain cellular telephones, including Apple iPhones, may be locked and/or unlocked by personal identification numbers (PIN), gestures or motions, and/or with biometric features, such as thumb and fingerprint recognition (collectively, “fingerprint ID”) and/or facial recognition (“facial ID”).

14. If a user enables the fingerprint ID unlock feature on a device, he or she can register several fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s sensor, which typically is found on the front of the device. In my training and experience, users of devices that offer fingerprint ID or facial ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

15. In some circumstances, a fingerprint or face cannot be used to unlock a device, and a passcode or password must be used instead. Depending on the configuration of the security settings on the phone, the opportunity to unlock the device via fingerprint ID or facial ID exists only for a short time. Fingerprint ID and facial ID also may not unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) several unsuccessful attempts to unlock the device are made.

16. The passcode or password that would unlock the device(s) found during the search is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) or present the face of the user(s) of the device(s) found during the search to the device’s fingerprint

ID or facial ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via fingerprint ID or facial ID is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

17. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a device via the fingerprints on thumbs or index fingers.

18. Based on the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Theretius GREENBERRY to the fingerprint ID sensor or to present his face to the facial ID sensor of any his seized device(s) to attempt to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

19. Based upon the above information, I respectfully submit that there is probable cause to search the item further described in Attachment A for the evidence further identified in Attachment B.